WRITTEN TESTIMONY OF

MARC J. ZWILLINGER, CISSP
NATIONAL CHAIR, INFORMATION SECURITY AND INTERNET ENFORCEMENT GROUP

Sonnenschein
SONNENSCHEIN NATH & ROSENTHAL LLP

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON MANAGEMENT, INTEGRATION AND OVERSIGHT
U.S. HOUSE OF REPRESENTATIVES

"The Need to Strengthen Information Security at the Department of Homeland Security"

APRIL 14, 2005

Sonnenschein
SONNENSCHEIN NATH & ROSENTHAL LLP

Written Testimony of Marc J. Zwillinger
April 14, 2005

Chairman Rogers, Ranking Member Meek, and Members of the Subcommittee, thank you for the opportunity to address the Subcommittee on the important topic of Strengthening Information Security at the Department of Homeland Security

Background

I have been a lawyer in the field of Information Security since 1997 when I was a Trial Attorney at the United States Department of Justice Computer Crime and Intellectual Property Section.

Since 2000, I have been leading an Information Security Legal practice at a national law firm. In my daily practice at Sonnenschein Nath & Rosenthal, I help private sector companies develop and maintain effective information security programs and incident response plans. While this may not be traditional legal work, I am not a traditional lawyer, as I am also a Certified Information Systems Security Professional and have training in computer forensics and network investigations.

In addition to my work with private companies, I have been part of two efforts to provide ideas to help secure the nation's critical infrastructure. First, I served as a member of the National Academies' Committee on Critical Information Infrastructure Protection and the Law. Second, I had the privilege of being invited to participate as the sole independent lawyer on the Corporate Information Security Working Group, which advised the House Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census. As with my testimony here today, my participation in both of those efforts was not on behalf of any client, but was an attempt to use my experience of representing clients in the information security space to help our country better protect its information assets.

Ironically enough, both of those prior efforts were geared towards finding better ways to motivate the private sector to protect the portions of the critical infrastructure under its control. However, now that a spate of industry-specific regulation and high-profile breaches of consumer information seem to be motivating the private sector to action, and given the Sarbanes-Oxley environment in which spending money on internal controls is becoming commonplace, it may be the public sector that could most benefit from additional attention.

About the Threats to Government Systems

When I was a computer crime prosecutor, it was conventional wisdom among hackers that government agencies and educational institutions were the low-hanging fruit of the computer world. These entities presented attractive targets because of the bandwidth and power of the computer systems available, and because the security at both types of institutions was ineffective.

When the focus of computer crime shifted away from the availability of computer resources to the market value of information stored on computer systems, the private sector became an interesting, and potentially lucrative, target.

But while that shift may have diminished the interest in hacking university systems (except as we have recently learned for the purpose of identity theft), government systems remain an attractive target for several reasons:

(1) the power and bandwidth of these computer systems;
(2) the critical nature of the information stored on such systems;
(3) the potential for significant disruption of critical government activities; and
(4) the inadequacy of security controls at many government agencies.

Of these factors, only the fourth is completely within the government's control. And the Federal Information Security Management Act (FISMA) was designed to change the way government agencies addressed this fourth factor. FISMA requires the head of each federal agency to provide information security protections that are commensurate with the risk and magnitude of harm that might result from unauthorized access, use, disclosure, modification or destruction of the information contained on such systems.

Changing the Risk Calculation

The same risk-based approach is contained in almost all information security legislation, regulations, and best practice guides that are used by the private sector, and always includes an assessment of the value of the information stored on the computer systems. What I have seen when counseling my private sector clients on information security issues, however, is that the motivation to improve information security relates not just to the value of the information at issue, but to several ancillary factors. In fact, private sector information may be less sensitive and present a lower risk of harm to the nation's security if compromised, but it is at times better protected than DHS information.

The risk that is evaluated and, with increasing frequency, acted upon by private corporations is the damage to the corporation's public reputation and the financial harm that may result. In fact, one of the key reasons that the private sector is sometimes predisposed against security breach notification legislation, such as the bills already introduced in the 109th Congress, is that when the risk of compromise of a system becomes the risk of public disclosure of that compromise, the consequences virtually demand a significant investment in security by every right-minded CEO or CIO of a public company for several reasons.

First, the public disclosure itself has the potential to drive down market value of a corporation. Second, disclosure of such breaches, irrespective of resulting harm,

tarnishes the corporation's reputation and interferes with customer relationships. Third, the public disclosure of breaches also creates an increased potential of litigation, threatening direct monetary loss as well as additional adverse publicity and lower market value.

As a result, these potential consequences are powerful enough to drive a corporation to invest in security even where the information stored is not as valuable as DHS data, because any breach directly threatens corporate financial results.

Lessons Learned

First, as I have described, risk assessments that focus solely on the value of the information to be protected have often been unsuccessful on their own in motivating good information security behavior. Accordingly, external forces caused a change in the risk calculus. But how do you change the risk calculus for the public sector?

FISMA report cards were designed to accomplish that objective. By identifying the agencies that were not meeting FISMA standards in a more public way than the detailed descriptions contained in the OMB reports, the associated stigma was intended to raise the profile of non-compliance, thereby creating incentive for action. However, absent a market value determination, the risk associated with receiving a failing grade is not nearly as catastrophic, nor as motivational, as it is in the private sector, even though the consequences of a compromise of DHS information may be greater.

Accordingly, FISMA compliance, and public sector information security in general, could be bolstered by offering incentives based on what we have seen work in the private sector. This includes responding to poor information security performance with stronger oversight or more exacting audits, and rewarding good security practices with positive incentives. It may also include tying security performance to the private sector equivalent of profit, namely funding. While it may seem offensive to suggest that the threat of a loss of our nation’s most sensitive and critical information is alone an insufficient incentive to improve information security, DHS's FISMA performance to date suggests that additional action may be warranted.

The second lesson is that many, if not most, of the breaches to which I have responded in the past four years have included compromises of data that was placed in the hands of third parties without a clear allocation of responsibility for security issues, or procedures for notification and response in the event of a breach. Given that of all the issues identified in OMB's 2004 FISMA report, DHS fared the best on "using appropriate methods to ensure that contractor-provided services are adequately secure," perhaps the private sector has something to learn from the government in this regard. On the whole, however, both sectors tend to worry less about data maintained by others, when the exact opposite should be true.

Third, as noted in the National Institute of Standards and Technology (NIST) Incident Handling Guidelines, "an incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computer services." In my experience with the private sector, organizations that have a robust incident response program not only catch incidents before they become serious, but in executing the incident response plan and remediating the vulnerabilities that are detected as a result of the plan, achieve a much improved security posture. DHS' poor performance on the FISMA categories of "tested contingency plans," and "effective security and privacy controls," suggests that either the Department's incident response plan is lacking, or its execution requires improvement.

Finally, Mr. Chairman, your Subcommittee would be hard-pressed to find too many security experts who would say that DHS is *saying* the wrong things. That is, instituting an Information Security Program Strategic Plan, working to institute DHS-wide policies within the organizational components, and collecting and verifying performance metrics are positive steps in the right direction. Nevertheless, the objective must be to create a culture of security within every organization, which clearly remains an evolving challenge in these early days of DHS.

My clients who have been successful at creating a culture of security can be easily distinguished from those that have not. For example, one of my clients flies in all of its product engineers, located domestically or internationally, for an annual multi-day conference on security issues, despite the time spent away from revenue-producing activities. In my view, that company clearly "gets it." Information security is not all about return on investment or liability prevention, rather, it is an essential component of their product development lifecycle and their culture. For the sake of the country, I would hope the same could be said about DHS in the very near future.

Mr. Chairman, again, thank you for your leadership in convening this important hearing and I stand ready to be of further assistance through answering your questions now or in the days ahead.